CITY AUDITOR'S OFFICE

IT Risk Assessment

June 14, 2016 REPORT NO. 1604

June 14, 2016

Honorable Mayor and Members of the City Council:

Enclosed is the *IT Risk Assessment* report, which replaced another contracted IT audit originally included on the Council-approved FY 2015/16 Audit Plan.

KPMG, under contract with and assisted by my office, performed the IT Risk Assessment. This assessment of the City's significant information systems (or applications) will provide a basis for identifying future IT audits. As well, the assessment process provides departments the opportunity to review their risk perspectives and approaches to mitigating risk.

If you need additional information or have any questions, please contact me at (480) 312-7867.

Sincerely,

Sharron Walker

Sharron E. Walker, CPA, CFE, CLEA
City Auditor

Audit Team:

Lai Cluff, Senior Auditor

TABLE OF CONTENTS

BACKGROUND

To avoid duplicating work being performed by a federal agency, this Information Technology Risk Assessment replaced the planned SCADA Network Contracted Audit on the Council-approved FY 2015/16 Audit Plan.

Objective, Scope and Methodology

The objective of the IT Risk Assessment was to gain an overall assessment of IT risk across the City's significant applications and the underlying technology infrastructure to use in planning future audits.

Using the Maricopa County contract for *Outside Audit, Cost Allocation, Grant/Program Support and Other Consulting Services*, we identified the firms approved for providing information technology audit services.[1] We developed a Task Order scope of work requesting proposals for an IT Risk Assessment, which was issued to the seven prequalified firms. Next, we evaluated the four competitive proposals received and selected KPMG to perform the work.

The scope of this risk assessment included major information systems currently being used by the following City departments.[2]

Departments Assessed
Airport
Court System
Planning and Development
Community Services
Fire Department
Police Department
Information Technology (Centralized IT)
City Treasurer's Office
Human Resources
Public Works

We identified the significant systems through past audits and inquiries of department staff. The assessed information systems included those used for cashiering, Police records management, Jail management system, the City's core financial system, the data backup system, traffic light management and others.

[1] The contract allowed cooperative use by members of the Strategic Alliance for Volume Expenditures (SAVE), which includes the City of Scottsdale.
[2] The term "department" will be used generically throughout this report to refer to department-level or division-level staff.

KPMG provided a questionnaire to collect preliminary information on each system, which we coordinated with the department IT staff. During May, KPMG and City Auditor staff met with IT staff for each of these departments to review the preliminary information and inquire further about potential risks and controls used for information system management. During these interviews, KPMG and staff reviewed key documents and discussed the characteristics, risks and controls for the various systems.

Based on the information system questionnaires, interviews and observations, KPMG provided its assessment of these applications' inherent and residual risks.

Inherent Risk – The susceptibility to risks, such as loss, misuse or error, before considering any related controls.

Residual Risk – The risk remaining after internal control processes are considered.

Assessment criteria for the inherent risk rating included:

Availability	Integrity	Security	Privacy	Confidentiality
•The risk associated with system downtime (e.g., hardware malfunctions, outages, disasters, etc.)	•The risk associated with corrupt, erroneous, inaccurate or incomplete data (e.g, algorithms, calculations, reports, etc.)	•The risk associated with unauthorized access to the system (both logical and physical)	•The risk associated with individuals, whether internal or external, gaining unauthorized access to sensitive data (e.g., credit card numbers, SSN, etc.)	•The risk associated with personal and non-personal data being disclosed without authorization

SOURCE: KPMG's identified criteria, based on the AICPA Trust Services core principles and criteria.

Next, threats were assessed to determine the likelihood of occurrence and magnitude of impact of the risks. Threats were compiled in the categories of man-made threats, natural threats or operational threats. Examples of these are illustrated on the next page.

Man-made Threats	**Natural** Threats	Operational Threats
•Denial or disruption of services •Inappropriate access of proprietary or private information •Insiders (e.g., poorly trained, disgrunteld, or terminated employees) •Modification or destruction (i.e., program code, networks, databases) •Terrorist acts	•Storms •Fires •Extreme heat •Dust storms •Drought/water supply •Lightning •Microbursts	•Dissatisfied citizens •Lack of funding •Lack of IT resources (staff or infrastructure) •Poor performance of 3rd party provider •Aging software or hardware •Computer attacks (e.g., viruses, spyware, adware, email hoaxes, SQL injections)

These threats were assessed using the following criteria for likelihood and magnitude.

> **Likelihood of occurrence** represents the probability that a potential vulnerability may be exercised by the threat source. A score ranging from 1 (remote) to 5 (imminent) was assigned to each.
>
> **Magnitude of impact** evaluates the adverse impact resulting from a vulnerability being exercised by a threat source. The inherent risk criteria (availability, security, etc.) were scored from 1 (minor) to 5 (severe) for magnitude of impact and these scores averaged.

Controls and mitigating factors identified through interviews were evaluated to determine a control score. Then residual risk was calculated by weighing the reported controls and mitigating factors against the inherent risk for each system. (The stated controls and mitigating factors were not tested as part of the risk assessment.)

KPMG's assessment ratings are summarized in the Results section of this report.

RESULTS

Risk assessment ratings represent a point-in-time as systems and operations continue to change on an ongoing basis. For example, the rated human resources/payroll system is slated to be replaced with a different application in the coming months. After being reviewed for any significant changes, these ratings will provide a basis for developing future IT audits.

Based on work performed during May 2016, KPMG summarized the IT risk ratings by Department as follows:

IT Applications for:	Average Inherent Risk	Average Residual Risk
Police Department		
Community Services		
Court System		
Fire Department		
Human Resources		
City Treasurer's Office		
Aviation		
City IT		
Public Works		
Planning		

High risk = >50.0 **Medium risk = 10.0 - 49.99** **Low risk = <10.0**

SOURCE: KPMG Risk assessment

(Continued on next page)

For individual applications, KPMG assessed the inherent and residual risks as follows:

#	Application Name	Average Inherent Risk	Residual Risk
1	Mobile Public Safety		
2	Computer Automated Dispatch		
3	Record Management System		
4	Zoi		
5	ActiveNet		
6	Jail Management System		
7	Commvault		
8	Lindsey Housing Manager		
9	Case Management System		
10	TotalHR		
11	Polaris		
12	Document Management		
13	Access Control Monitoring		
14	Airport System Operations Control		
15	NorthStar		
16	Risk Master		
17	ShieldScreening		
18	SmartStream		
19	iNovah		
20	HSCAMS		
21	GenTax		
22	Telestaff Scheduling		
23	Airport Business Manager		
24	Active Directory		
25	NetMotion		

(Continued on next page)

#	Application Name	Average Inherent Risk	Residual Risk
26	Fire Records		
27	Outlook		
28	Fire Prevention RMS		
29	Chameleon		
30	Cherwell		
31	Transcore		
32	Velocity		
33	Community Development System (CDS)		
34	Scottsdale University		

High risk = >50.0 **Medium risk = 10.0 - 49.99** **Low risk = <10.0**

SOURCE: KPMG Risk assessment

In addition to the risk assessment ratings, KPMG also reported a few high-level observations. These included the following:

Observation	Description
Policies and Procedures	There are formally approved and administered policies for key IT processes throughout the City. However, it appears these policies are not communicated to individual IT groups within several departments.
Vendor Management	Areas relying on 3rd party hosted and/or managed applications are not periodically reviewing attestation reports on the reliability and effectiveness of controls.
Disaster Recovery Plan (DRP)	A Citywide DRP is being implemented, including a secondary failover location. Given the current infrastructure coupled with high availability impact for several applications, without a documented and tested DRP an outage could result in a critical incident and/or prolonged outage of critical systems.
Staffing	IT resources are limited by department. In instances where applications are managed in-house and not by a vendor or the centralized IT department, the departmental IT staff is often managing multiple applications with little to no assistance. Furthermore, the resources are not always skilled IT professionals but instead have been trained to manage their particular system.

City Auditor's Office
7447 E. Indian School Rd., Suite 205
Scottsdale, Arizona 85251

OFFICE (480) 312-7756
INTEGRITY LINE (480) 312-8348

www.ScottsdaleAZ.gov/auditor

The City Auditor's Office conducts audits to promote operational efficiency, effectiveness, accountability, and integrity.